Journal of
Cyber Security

Tech Science Press

https://doi.org/10.32604/jcs.2026.077850

REVIEW

Intrusion Detection Systems from IT to IIoT: Survey and Taxonomy

Ali Lamjid[1,*], **Khairul Akram Zainol Ariffin**[1,*], **Mohd Juzaiddin Ab Aziz**[2] **and Nor Samsiah Sani**[3]

[1]Center for Cybersecurity, FTSM, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia
[2]Center for Software Technology and Management, FTSM, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia
[3]Center for Artificial Intelligence and Technology, FTSM, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

*Corresponding Authors: Ali Lamjid. Email: ali.lamjid@gmail.com; Khairul Akram Zainol Ariffin. Email: k.akram@ukm.edu.my

Received: 18 December 2025; Accepted: 06 March 2026; Published: 25 May 2026

ABSTRACT: The convergence of Operational Technology (OT) and Information Technology (IT) within Critical Infrastructures gives rise to complex and heterogeneous network architectures in the Industrial Internet of Things (IIoT). Traditional Intrusion Detection Systems (IDS), designed for conventional IT environments, are suited for mitigating vulnerabilities inherent in these systems; however, they often fail to address vulnerabilities intrinsic to heterogeneous IIoT architectures, most notably adversarial threats. To address this challenge, this study undertakes a systematic review of 23 representative papers published between 2016 and 2025, analyzing the IIoT-based IDS approaches. Distinguishing itself from existing reviews, this work classifies IDS approaches based on deployment architecture, detection methodology, and security threat types, thereby identifying a critical gap in current defensive capabilities. This analytical framework reveals a critical deficiency in current defense mechanisms against sophisticated threats such as adversarial attacks. The proposed taxonomy provides a foundational framework for the rational design of robust hybrid IDS solutions that can secure both legacy supervisory control and data acquisition (SCADA) systems and modern smart devices. Ultimately, these findings provide a strategic road-map for researchers and practitioners to advance Cybersecurity resilience in the rapidly maturing IIoT platforms.

KEYWORDS: Cybersecurity; intrusion detection system; IT; OT; industrial IoT; taxonomy

1 Introduction

IIoT emerges from the convergence of IT and OT. While IT encompasses the data processing capabilities of standard computer networks, OT pertains to the monitoring and control of physical processes within industrial control systems (ICS), encompassing the hardware and software that manage critical infrastructures (CI) and industrial facilities. Consequently, ensuring the security, integrity, and most critically within OT environments, availability of data flows across interconnected industrial networks is imperative. IDS, implemented in both software and hardware forms, serves as a foundational tool for securing the IIoT. As emphasized by [1], IDSs are engineered to monitor network activity in real time and respond to security threats, rendering them indispensable components of IIoT security architectures.

Within the broader Cybersecurity landscape, numerous defensive strategies have been developed to mitigate breaches and emerging threats. Among these, IDSs represent a robust and widely researched defensive mechanism. Research indicates that IDSs are primarily designed to automatically identify malicious software [2] and distinguish legitimate traffic through continuous host and network flow monitoring [3]. Furthermore, IDSs have become essential for safeguarding IoT ecosystems against Cyber-attacks [4]. Nevertheless, conventional IDS frameworks are increasingly inadequate against novel and sophisticated attack

Copyright © 2026 The Authors. Published by Tech Science Press. This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

vectors due to their reliance on signature-based detection [5]. As noted by [6], this signature-dependent paradigm inherently limits the capacity of traditional IDSs to identify anonymized or evasive attacks.

Existing Cybersecurity research has extensively explored IDS classifications based on data flow analysis and device configuration. In the context of industrial IoT, IDS categorization is particularly multifaceted, with numerous systems tailored to specific communication technologies [7]. However, directly transplanting traditional IT-centric IDS architectures into IIoT environments frequently proves ineffective. The distributed topology of IIoT networks, coupled with heterogeneous systems, proprietary protocols, and resource-constrained devices, significantly impairs the threat detection capabilities of legacy IDS solutions [8]. While IIoT deployment substantially optimizes industrial control and monitoring processes [9], the concurrent proliferation of sensor-generated data creates an expanded attack surface that actively attracts malicious actors [10].

As IIoT security increasingly leverages ML and DL for intrusion detection, adversarial machine learning has emerged as a tangible threat. Attackers can exploit evasion techniques by crafting malicious traffic that mimics benign traffic patterns or by employing poisoning strategies to corrupt training datasets, thereby degrading model performance. Although adversarial threats have been investigated within broader IoT and Cyber-physical systems (CPS) research [11–13], they remain conspicuously underrepresented in contemporary IDS taxonomies and survey-driven classification frameworks.

Designing an effective IDS for IIoT environments is therefore highly complex. It requires securing distributed, heterogeneous devices with unique operational constraints while simultaneously addressing the novel threat vectors introduced by the pervasive integration of internet connectivity into industrial infrastructure. To bridge these gaps, recent research has introduced specialized IDS architectures customized to specific industrial environments and communication mediums. Moreover, emerging high-efficacy intrusion methodologies, particularly adversarial threat models, must be systematically integrated into detection frameworks to enhance both academic comparability and practical system design.

This study aims to comprehensively review IDS methodologies across IT, IoT, and IIoT domains, subsequently proposing a unified taxonomy that generalizes existing IDS classifications and addresses identified research gaps to strengthen IIoT infrastructure security.

Consequently, the primary contributions of this paper are summarized as follows:

1. It synthesizes IDS research across IT, IoT, and IIoT/ICS settings, emphasizing how industrial segmentation, protocol diversity, and OT safety/availability constraints affect IDS design and deployment.
2. It presents a transparent review process and comparative synthesis of representative studies (2016–2025) to identify dominant trends (e.g., anomaly-based detection) and persistent gaps (e.g., adversarial robustness).
3. It proposes a new IIoT-oriented IDS taxonomy that extends existing classifications by incorporating operational dimensions (deployment architecture, mode, response behavior, and output granularity) and explicitly introducing attack nature, including adversarial attacks.

The remainder of this paper is organized as follows: Section 2 reviews prior Cybersecurity research pertaining to industrial platforms. Section 3 examines prevailing IDS methodologies. Section 4 introduces the proposed taxonomy and its application across diverse IIoT scenarios. Section 5 presents the study's conclusions, and Section 6 outlines directions for future research.

2 Literature Review

The Cybersecurity research landscape pertaining to the IIoT has evolved from broad taxonomic surveys toward specialized literature reviews emphasizing advanced computational paradigms. While this scholarly

effort has substantially advanced technical understanding, the resulting body of knowledge remains highly fragmented, failing to comprehensively address the stringent operational constraints and heterogeneous reality of IIoT environments. A critical examination of the literature reveals distinct research clusters, each demonstrating notable strengths yet exhibiting specific, frequently overlooked limitations regarding IIoT security.

Foundational surveys established essential categorization frameworks for threats and IDS within IoT and IIoT ecosystems. Seminal works by [1,13,14] developed comprehensive taxonomies for attack vectors and corresponding mitigation strategies, serving as benchmark references that standardized terminology across an otherwise fragmented domain. However, these early surveys exhibit a notable limitation: insufficient coverage of ML and DL techniques, which have since become indispensable for addressing the escalating volume and diversity of Cyber-threats [15]. Furthermore, they frequently treat IIoT as a mere extension of conventional IoT, thereby overlooking the stringent reliability, safety, and integrity requirements inherent to OT environments [14].

A subsequent and highly prominent body of literature concentrates extensively on ML and DL methodologies for intrusion detection. Comprehensive reviews by [3,5] systematically evaluate algorithmic approaches, ranging from classical statistical models to advanced neural architectures such as CNNs and RNNs. While these studies excel in benchmarking model accuracy and performance on standardized datasets, their applicability to IIoT contexts is limited by three critical shortcomings. First, they prioritize algorithmic complexity over practical deployability on resource-constrained edge devices, which constitute a defining characteristic of IIoT networks [11]. Second, they largely overlook the necessity of Explainable AI (XAI), a crucial requirement in industrial settings where operators must comprehend and trust automated alarm responses to enable effective intervention [15]. Third, they frequently disregard adversarial machine learning threats, wherein attackers deliberately craft inputs to evade detection; a vulnerability that poses severe risks to critical infrastructure [16,17].

Concurrent with algorithmic-focused reviews, several studies propose integrated architectural frameworks tailored to specific industrial sectors, particularly smart grid infrastructures. Frameworks such as SPEAR [18] and ELECTRON [19] exemplify this approach by unifying intrusion detection, forensic readiness, and autonomous self-healing capabilities into cohesive security architectures.

Additionally, domain-specific taxonomies have been developed for specialized environments, including supervised learning frameworks for SCADA systems [20]. Nevertheless, these classifications rarely address the IIoT ecosystem holistically. Similarly, while research on adversarial attacks [11] is highly pertinent, it remains isolated within specialized literature streams and has yet to be systematically integrated into mainstream IIoT IDS classification schemes.

This critical synthesis underscores a pronounced fragmentation within the existing literature. Specifically, four persistent research gaps hinder the development of effective IIoT security solutions: 1) The Deployment Gap: a scarcity of lightweight, hardware-efficient DL models optimized for resource-constrained IIoT edge layers, 2) The Resilience Gap: the insufficient integration of adversarial robustness and privacy-preserving mechanisms into foundational IDS design taxonomies, 3) The Operational Gap: the lack of unified frameworks that synergize IT-centric detection methodologies with OT-driven physical process monitoring, and 4) The Validation Gap: an over-reliance on generic IoT datasets, coupled with a notable absence of standardized, OT-specific benchmarking environments for empirical validation.

Thus, synthesizing these disparate research streams establishes a clear rationale for a novel, unified taxonomy. A contemporary IIoT IDS classification framework must transcend isolated specializations by

categorizing detection approaches not solely by algorithmic methodology (e.g., signature-based, anomaly-based, hybrid, or specific ML/DL architectures such as SVM, CNN, and LSTM), but also by deployment paradigm (edge, cloud, or hybrid), resilience attributes (adversarial training, privacy-enhancing technologies, and explainability levels), and legacy OT integration strategies. Such a multidimensional framework will effectively bridge the divide between theoretical algorithmic performance and the practical requirements of secure, trustworthy, and deployable solutions in operational industrial environments. Ultimately, this structured approach is designed to guide future research toward the development of more holistic, standardized, and practically applicable IIoT Cybersecurity methodologies.

3 IIoT and Related Cyberattacks

The IIoT represents the adaptation of IoT technologies within industrial infrastructures. Sensor-collected data are processed and distributed to end-users, while command signals from management centers are relayed to actuators and underlying device systems. At the physical level, devices are interconnected via communication networks, enabling data exchange across applications through cloud-based big data analytics. Fig. 1 illustrates the propagation and processing of data within the IIoT architecture.

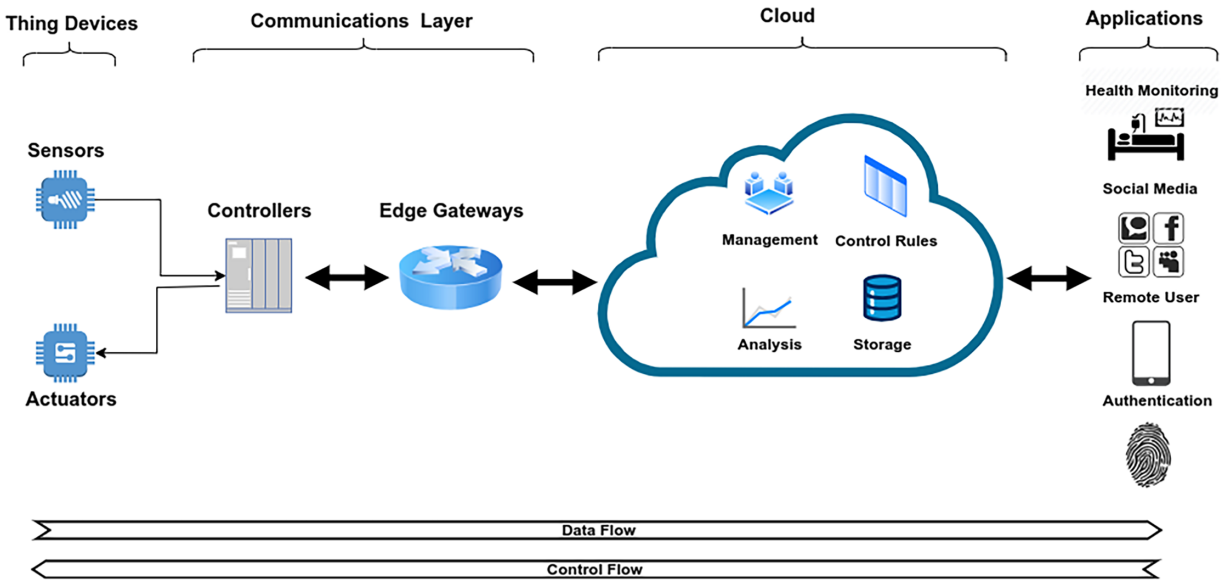

Figure 1: Data flow in different parts of the IIoT.

The primary objective of IIoT deployment is to enhance operational productivity and economic efficiency. Consequently, securing both the IIoT platform and the bidirectional flow of information is critical. However, the distributed and decentralized nature of IIoT devices complicates security enforcement. Furthermore, the continuous scalability of IIoT infrastructure necessitates ongoing security enhancements. Each newly integrated component introduces unique data-processing requirements, and this growing heterogeneity must be effectively managed [21]. Due to their inherently heterogeneous architecture, IoT and IIoT platforms remain susceptible to multiple vulnerabilities. System integrity is frequently compromised by issues such as unsecured wireless transmission and the injection of falsified data into the network [22].

The expansion of IIoT architectures across multiple structural levels introduces diverse vulnerabilities that adversaries exploit through various attack vectors. In this context, [15] categorizes threats according to the five-layer IIoT architecture detailed in Table 1. These attacks are classified into two domains: the upper

two layers correspond to conventional Information Technology (IT), while the lower three layers align with Operational Technology (OT), the industrial counterpart to traditional IT systems.

Table 1: Possible attacks in IIoT for each layer.

		Layers	Components	Possible Attacks
IT	5	Business Layer	Business Applications, Internet, Cloud Computing, Data Analytic, mobile Devices.	DoS, side channel attacks, Cloud malware Injection, Authentication attacks, Man in the Middle, Mobile device attacks.
	4	Application Layer	Data Centers, Intranet, Mail, Office Applications, Web Services.	Phishing, Malware, DNS, SQL Injections, poisoning, Brute Force attack, Remote code Execution, Web Application attacks.
			Demilitarized zone	
OT	3	Processing Layer	SCADA Control, HMI, Control Room, Operator Stations.	IP spoofing, Data manipulation, Data sniffing, Malwares.
	2	Transport Layer	Distributed Control System, PLC, Gateways.	Replay attack, Sniffing, Man-in-the-Middle attack, Brute force Password guessing, Wireless device attack.
	1	Perception Layer	Sensor, Motors, Actuators, Transmitters, Embedded Devices.	Reverse Engineering, injecting crafted packages or input, Malware, Eavesdropping, Brute force search attacks.

These two domains are separated by a DeMilitarized Zone (DMZ), an isolated network segment that hosts externally accessible servers while preserving the security of the core infrastructure. The DMZ restricts direct, unrestricted connectivity between IT and OT networks, thereby mitigating cross-domain compromise [23].

The first level (Perception Layer): Comprises physical devices such as sensors and actuators. Due to their reliance on wireless communication, these components are susceptible to signal jamming, eavesdropping, and physical tampering, which can introduce falsified data into the control loop [24].

The second level (Transport Layer): Encompasses edge controllers, routers, and programmable logic controllers (PLCs). This layer bridges physical devices with the internet. Weak encryption on network gateways can enable Man-in-the-Middle (MitM) attacks or the interception of control commands [25].

The third level (Control Layer): Integrates SCADA systems and operator workstations. Functioning as the central nervous system of OT environments, this layer is a primary target for malware injection within industrial networks. Compromise at this level can result in loss of situational awareness for operators or direct loss of control over industrial processes [26].

The fourth level (Application Layer): Manages industrial software applications and services. Utilizing standard IT protocols such as HTTP and SQL, this layer remains vulnerable to conventional web-based threats, including SQL injection and phishing, which can lead to data exfiltration or remote code execution [27].

The fifth level (Business Layer): Provides data analytics and business intelligence to end-users. Integration with third-party partners and cloud-based services expands the attack surface, elevating the risk of sensitive data leakage and strategic espionage [28].

Furthermore, the proliferation of artificial intelligence (AI) has introduced novel attack methodologies targeting data-driven systems. While [29] identifies adversarial attacks as advanced threats primarily targeting the business layer, and [11] concentrates on sensor-level exploits within the perception layer, adversarial sample generation remains feasible across any data-processing environment, independent of architectural tier [12].

The efficacy of an adversarial attack hinges on the adversary's capacity to manipulate the feature distributions and class boundaries of training or inference data acquired across heterogeneous IoT/IIoT infrastructures. Defending neural networks against such threats using traditional perimeter defenses like firewalls is inherently difficult, as these vulnerabilities stem from mathematical optimization properties rather than network topology or protocol flaws. Conventional IDS frameworks operate on deterministic rule-matching logic, whereas AI-driven IDS relies on probabilistic inference. As demonstrated by [30], adversarial examples are constructed by applying imperceptible perturbations to input data, which remain undetectable to human observers yet induce severe model misclassification. Within IIoT environments, this capability is particularly catastrophic. Adversaries no longer require traditional software vulnerabilities such as buffer overflows; instead, they merely compute the optimal mathematical gradient that forces a neural network to misclassify a malicious payload as benign traffic.

4 Defense Mechanism in the IDS Approaches

Intrusions can be devastating to industrial infrastructure. Numerous surveys and reviews have been conducted in the IDS domain to enhance CI cybersecurity. The primary objective of this research is to analyze various IDS approaches across different environments and infrastructures, culminating in the development of a novel taxonomy. The key contributions of this study are as follows: (i) A systematic review of recent literature (2016–2025) focusing on IDS applications in CI, IT networks, and IIoT infrastructures; (ii) A comprehensive evaluation of the selected articles from the perspective of designing specific IDS approaches, including a critical assessment of their methodologies; and (iii) The identification and categorization of various IDS techniques, leading to the proposal of a new taxonomy that addresses existing gaps in IDS research for handling emerging threats, such as adversarial attacks.

This analysis highlights the most commonly used types of IDSs, including anomaly-based, misuse-based, host-based, network-based, and hybrid IDSs, which represent the predominant strategies in cybersecurity intrusion detection.

This review was conducted in three phases. In Phase 1, relevant articles were identified through academic databases and publisher platforms, including Elsevier, Springer, IEEE Xplore, ACM Digital Library, Wiley, Taylor & Francis, MDPI, arXiv, and Google Scholar. A targeted keyword search combining terms such as "IDS," "GAN," "adversarial attacks," "cybersecurity," "IIoT," "IoT," and "critical infrastructures" yielded a preliminary collection of articles (List 1). In Phase 2, the articles were categorized according to their primary application domain, such as traditional IT networks, IoT, IIoT, or other related areas. In Phase 3, the collection was refined by retaining only studies that explicitly proposed or evaluated an IDS methodology

(forming List 2), while excluding general cybersecurity papers that lacked a specific IDS approach. Fig. 2 illustrates the systematic review workflow employed to evaluate the various IDS approaches discussed in this research.

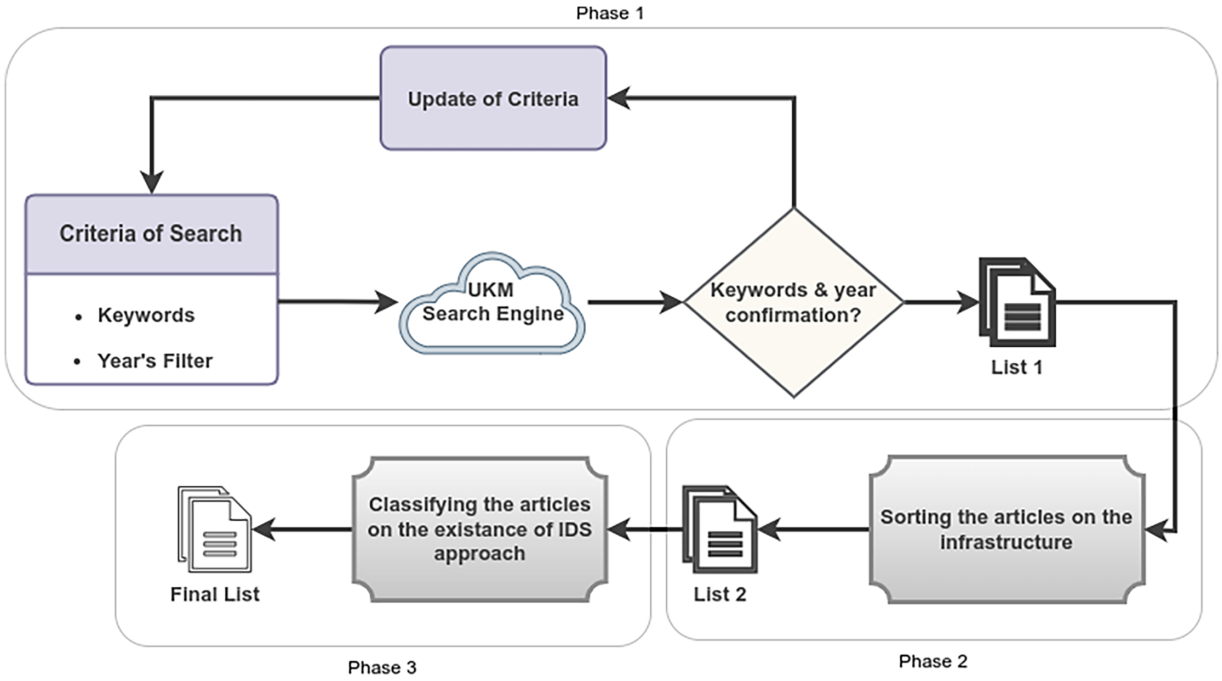

Figure 2: Research papers process flow.

A comprehensive review of intrusion detection literature was conducted by systematically analyzing publications retrieved from major academic databases and digital repositories. From this corpus, 23 representative studies were selected based on their widespread adoption in both contemporary IDS research and practical deployments. These selected works encompass three primary dimensions: (a) core detection paradigms (signature-based, anomaly-based, specification-based, and hybrid), (b) deployment architectures (host-based, network-based, and distributed), and (c) target environments (IT networks, IoT, ICS/SCADA, and IIoT). Host-based IDS (HIDS) monitors system logs and events on individual devices—such as servers, endpoints, and PLC-adjacent hosts—offering fine-grained visibility at the cost of limited network-wide coverage. Conversely, network-based IDS (NIDS) [3] inspects packet/flow data to observe inter-device communications, though it must contend with encrypted traffic, high throughput demands, and protocol heterogeneity. Signature-based detection remains highly efficient against known threats but struggles with zero-day and evolving attacks.

In contrast, anomaly-based detection, increasingly powered by machine learning and deep learning, dominates recent literature due to its adaptability to heterogeneous IoT/IIoT traffic patterns [15,31,32]. Specification-based approaches, particularly prevalent in ICS/SCADA environments, leverage predefined protocol and process invariants to minimize false positives when operational rules are well established. Hybrid IDS architectures integrate multiple paradigms to enhance detection coverage, proving especially valuable in environments facing both known malware and novel behavioral anomalies. Across the reviewed literature, a clear paradigm shift is evident: the field is moving away from static signature matching toward adaptive anomaly detection and hybrid frameworks. However, this evolution introduces new vulnerabilities, particularly adversarial machine learning attacks and model fragility. Consequently, a robust IIoT-oriented

IDS taxonomy must extend beyond traditional classifications of placement and detection logic. It should also incorporate operational modes, response behaviors, output granularity, and adversarial threat modeling. To address this need, this study proposes a novel taxonomy that systematically categorizes IDS techniques according to their detection mechanisms, data sources, and deployment architectures. By mapping the evolution of intrusion detection methodologies and highlighting emerging trends, this classification system establishes a structured foundation for future research, cross-methodological evaluation, and the development of more resilient cybersecurity solutions.

Ref. [33] frames intrusion detection as a binary classification task that distinguishes normal traffic from anomalous patterns. The study emphasizes that rigorous feature selection can significantly enhance classifier performance, improving detection rates and accuracy while reducing false positives and computational overhead. It also identifies promising future directions, particularly the development of novel feature selection methods leveraging robust metaheuristic optimization algorithms.

Ref. [24] surveys IDS architectures tailored to IoT environments, detailing mechanisms for mitigating various IoT-specific attacks. The authors underscore the critical importance of cybersecurity in IoT, addressing core security properties such as confidentiality, integrity, availability, authenticity, non-repudiation, and data freshness. While IDS is commonly deployed as a secondary line of defense, the study notes that existing solutions often struggle to detect the full spectrum of cyber threats due to high computational, memory, and bandwidth demands. Consequently, the authors recommend developing lightweight, resource-efficient detection mechanisms for constrained IoT deployments.

Drawing on 18 studies, [8] presents a comprehensive survey of IoT-based IDS, categorizing approaches across four dimensions: deployment strategy, detection methodology, targeted security threats, and validation techniques. This work proposes a taxonomy mapping the various IDS techniques applied in IoT ecosystems. However, the proposed framework does not fully address the complete range of cyberattacks or account for the diverse network topologies inherent to modern IoT deployments.

Ref. [25] offers a detailed review of both Intrusion Detection Systems (IDS) and Intrusion Response Systems (IRS). The study catalogs the types of intrusions detectable by IDS architectures and outlines corresponding response strategies. IDS are classified into four primary categories: host-based, network-based, hybrid, and distributed. Correspondingly, IRS are categorized into active and passive response mechanisms. The authors highlight a critical research gap: automated IRS requires further development to enable timely, adaptive threat mitigation.

Ref. [26] examines diverse IDS typologies, analyzing their underlying platforms and the attack vectors they are designed to detect across different operational environments. The review covers host-based, network-based, protocol-based, application-based, hybrid, and virtual machine introspection (VMI)-based IDS. The study concludes with a comparative analysis evaluating the strengths, limitations, and deployment trade-offs of each IDS category.

Ref. [2] observes that conventional IDS architectures are primarily optimized for traditional IT environments, necessitating a taxonomy that accounts for the unique operational constraints of Industrial Control Systems (ICS). To address this gap, the authors propose a novel ICS-focused taxonomy grounded in protocol analysis, traffic mining, and control-process modeling. Additionally, the study evaluates the advantages and limitations of various IDS types when deployed within ICS environments.

Ref. [1] addresses the expanding IoT attack surface driven by the proliferation of remotely connected devices. Moving beyond traditional IDS paradigms, the study proposes a behavior-based detection framework that captures device telemetry through tracing mechanisms. These behavioral profiles are then used to train machine learning models, with the proposed solution validated in a home automation testbed.

Ref. [27] notes that while numerous IDS rely on signature-based, supervised learning, or statistical methods, their reliability remains constrained by limited generalization to emerging threats. As the complexity and frequency of modern attacks have escalated, conventional approaches have proven insufficient, prompting a shift toward feature-engineering-driven methodologies that enhance detection adaptability and robustness.

Ref. [28] surveys IDS architectures tailored for IoT-based smart environments. The authors note that while numerous IDS solutions have been designed for IoT models, there remains a critical need for efficient, reliable, and robust detection systems capable of addressing the unique vulnerabilities across different IoT architectural layers. Consequently, the study identifies key research directions to advance IoT-focused IDS development.

Ref. [34] examines the role and significance of IDS in securing IoT ecosystems. The study provides a comprehensive analysis of existing IDS solutions, evaluating their effectiveness in mitigating cybersecurity threats while addressing challenges related to transparency and resource constraints. The authors categorize prior IDS classifications by detection methodology and targeted security threats, highlighting the limitations of studies that focus narrowly on specific IoT security aspects. To address these gaps, they propose a software-defined IDS deployed on a distributed cloud framework, demonstrating improved detection accuracy compared to traditional approaches.

Ref. [3] presents a comprehensive review of machine learning (ML) and deep learning (DL) applications in network intrusion detection systems (NIDS). The study details the methodologies employed in each reviewed work, identifies limitations in existing IDS implementations, and analyzes the selection criteria for ML/DL algorithms alongside standard evaluation metrics using benchmark datasets. The authors conclude that while DL algorithms achieve high detection efficiency, they often incur significant computational overhead during deployment.

Ref. [20] outlines a practical framework for implementing cybersecurity standards and mitigation strategies to protect machine-to-machine (M2M) communications in IIoT environments. The authors propose an IIoT-specific cybersecurity taxonomy that details industrial control system (ICS) vulnerabilities, potential cyber threat consequences, and broader security challenges. This work emphasizes the need for tailored security mechanisms to address the unique operational constraints of IIoT networks.

Ref. [35] Reviews IDS deployment strategies in IoT environments, highlighting their limitations in comprehensively identifying IoT-specific threats due to architectural constraints. The study explores the application of ML and DL techniques to enhance IDS effectiveness, analyzing relevant datasets, common IoT attack vectors, and existing taxonomies. The authors also propose an expanded attack classification framework to better align IDS design with emerging IoT threat landscapes.

The taxonomy proposed by [36] specifically addresses IDS designed for SCADA environments, categorizing systems based on three core dimensions: (i) Function-Centric, which focuses on operational SCADA processes and alarm generation for parameter deviations (both expected and anomalous); (ii) Data-Centric, which classifies detection approaches based on the data sources and types utilized; and (iii) Architecture-Centric, which evaluates IDS deployment models and integration strategies within SCADA networks. The authors emphasize that securing SCADA systems is particularly challenging due to their dual exposure to IT and OT vulnerabilities.

Ref. [37] addresses cloud computing security, focusing on IDS classification by attack type, deployment location, and configuration. The study places particular emphasis on virtual machine and hypervisor introspection techniques. Additionally, it identifies key security concerns, underscores the importance of feature selection and dimensionality reduction, and outlines critical research gaps for future investigation.

Ref. [38] examines the challenges of intrusion detection in computer networks and IoT infrastructures, noting that conventional algorithms often struggle against sophisticated, evolving threats. The authors analyze publicly available network datasets and evaluate the performance of DL-based automated IDS. The study concludes by outlining current challenges and promising solutions for enhancing network security.

Ref. [7] provides a comprehensive overview of cybersecurity challenges in industrial IoT (IIoT) and their implications across various industries. The review focuses on the implementation of DL techniques for IIoT IDS development, detailing associated opportunities, technical hurdles, and deployment considerations.

Ref. [39] addresses the interpretability challenges cybersecurity professionals face when analyzing outputs from DL-based IDS, which are often treated as black-box models. To mitigate this, the study surveys existing explainable IDS (X-IDS) frameworks designed to justify detection predictions. The authors also propose a generalized X-IDS architecture and outline research directions to enhance model transparency and trustworthiness.

Ref. [40] discusses IoT security challenges and presents a comparative taxonomy of existing IDS approaches. To address limitations in prior research, the authors propose an intelligent IDS that integrates a convolutional neural network (CNN) with fuzzy logic rules. Feature selection is optimized using the information gain ratio to enhance detection efficiency. The study synthesizes findings from multiple sources to validate the proposed approach.

Ref. [41] investigates the application of DL in IoT-based IDS, focusing on detection accuracy and dataset imbalance challenges. The authors survey techniques and methodologies designed to improve DL model performance in this domain. While noting significant progress, the study emphasizes the need for further research to address scalability, generalization, and real-world deployment, offering actionable recommendations for future work.

Ref. [42] highlights the critical role of high-quality datasets in developing effective IDS for software-defined networking (SDN) environments. The study emphasizes the need for innovative security mechanisms tailored to SDN architectures to counter evolving cyber threats. Focusing specifically on SDN-based IDS, the authors propose a dedicated taxonomy to guide future research and development.

Ref. [43] explores the intersection of security and energy efficiency in IoT devices. The authors examine various strategies for implementing energy-aware security across management, application, network, hardware, and software layers. The study stresses the importance of context-aware security mechanisms that dynamically adapt to environmental conditions and evolving threat levels.

Ref. [44] conducts a systematic literature review of host-based intrusion detection systems (HIDS) from 2020 to 2023, analyzing 21 studies and evaluating their detection methodologies. The review identifies key limitations in current research, including insufficient real-world validation, reliance on outdated datasets, and a lack of emphasis on real-time monitoring capabilities.

Table 2 summarizes the IDS approaches discussed in the previously reviewed literature.

Table 2: Different IDS strategies in the literature.

	Author	Type of IDS	Level 1	Level 2	Level 3
1	Acharya and Singh, 2016 [33]	IDS	Based on the Type of attacks	Host based	
				Network based	
			Based upon the solution techniques	Anomaly detection	
				Misuse detection	
			Based upon the behaviour	Active	
				Passive	

(Continued)

Table 2 (continued)

	Author	Type of IDS	Level 1	Level 2	Level 3
2	Sherasiya et al., 2016 [24]	IDS Approaches	Rule-Based		
			Anomaly Based		
			Hierarchical Energy Efficient Based		
			Distributed Detection Based		
			Cluster-Based		
			Hybrid		
3	Zarpelão et al., 2017 [8]	IDS for IoT	Placement strategies	Distributed	
				Centralized	
				Hybrid	
			Detection method	Signature Based	
				Anomaly Based	
				Specification Based	
				Hybrid	
			Security threat	Conventional Attack	
				Routing Attack	
				Man in The Middle	
				DoS	
			Validation strategy	Hypothetical	
				Empirical	
				Simulation	
				Theoretical	
				None	
4	Anwar et al., 2017 [25]	IDS types	Host-Based		
			Network-Based		
			Hybrid		
			Distributed		
5	Othman et al., 2018 [26]	Classification of IDS Types	Host	Host Based	
			Network	Network Based	
				Network Behaviour Analysis	
				Wireless IDS	
				Distributed and Collaborative IDS	
			Hybrid	Hybrid Based	
				Protocol Based	
				Database IDS	
			Virtual Machine	Hypervisor Based	
6	Hu et al., 2018 [2]	IDS for ICS	protocol analysis-based,		
			traffic mining-based		
			control process analysis-based		
7	Gassais et al., 2020 [28]	IDS in IoT	Anomaly Detection	Classification	
				Clustering	
				Statistics	
			Tracing and debugging embedded device		

(Continued)

Table 2 (continued)

	Author	Type of IDS	Level 1	Level 2	Level 3
8	Nisioti et al., 2018 [27]	General Classification of IDS	Implementation method	Host-based	
				Network-based	Packet-based
					Flow-based
				Hybrid	
			Architecture	Centralized	
				Decentralized	
				Distributed	
			Detection method	Signature-based	
				Anomaly-based	Supervised
					Unsupervised
					Semi-supervised
					Hybrid
				Hybrid	
9	Elrawy et al., 2018 [1]	IDS	Types and methods	host-based	
				network-based	
			Detection techniques	Misuse-based	
				Anomaly-based	Data mining
					Machine learning
					Statistical mode
					Rule model
					Payload model
					Protocol model
					Signal processing model
			Specification-based		

(Continued)

Table 2 (continued)

	Author	Type of IDS	Level 1	Level 2	Level 3
10	Sicato et al., 2020 [34]	IDS for IoT	Detection Method	Anomaly Based	Supervised ML based technique
					Unsupervised ML based technique
				Network Based	
				Host Based	Using anomaly & signature based technique
					Using both & specification based technique
				Distributed Based	
			Security Threat	Denial of Service	Volume based attacks
					Protocol attacks
				Man in The Middle	
				Routing Attacks	Sybil attacks
					Worm hole attacks
11	Ahmad et al., 2021 [3]	IDS	Deployment Method based IDS	Host based	
				Network based	
			Detection Method based IDS	Signature based IDS	
				Anomaly Detection based IDS	
12	Suaboot et al., 2021 [20]	IDS for SCADA	Function-centric	Automatic response	
				Notification only	
			Information-centric	Host based	
				Network based	
			Analysis-centric	Anomaly based	
				Signature based	
13	Khraisat and Alazab, 2021 [35]	IDS for IoT	Placement Strategy	Distributed Centralized Hybrid	
			Detection Method	Signature Based	
				Anomaly Based	
				Hybrid	
			Validation Strategy	Simulation	
				Theoretical	
				Empirical	
				Hypothetical	
				None	

(Continued)

Table 2 (continued)

	Author	Type of IDS	Level 1	Level 2								Level 3		
				IT Focus								OT Focus		
				Confidentiality			Availability					Integrity		
14	Dhirani et al., 2021 [36]	Cybersecurity taxonomy for IIoT	Cyber Threats	Eavesdroping/ Interception	Nefarious activity		Outages	Disaster	Failures or malfunctions			Legal	Unintentional damage Physical attacks	
			Cybersecurity issues	Data Security	Communications and securityre-quirements		Security controls and standardisation	Visibility insights and control	It/OT Convergence			Threat intelligence	Outdated systems	Service level agreements
15	Lata and Singh, 2022 [37]	IDS Techniques	Signature Based											
			Anomaly Based				Artificial Neural Network							
							Support Vector Machine							
							Genetic Algorithm							
							Fuzzy Logic							
							Associated Rule Mining							
			Hypervisor Introspection											
			Virtual Machine Introspection				Memory Introspection							
							I/O Introspection							
							Process Introspection							
			Hybrid Techniques											
16	Khan et al., 2022 [38]	IDS	Signature-Based Intrusion Detection Systems											
			Anomaly-Based Intrusion Detection System											
			Customized Intrusion Detection Methods											
			Hybrid Intrusion Detection Methods											
			Host-Based IDS											
			Network-Based IDS											
			Distributed IDS											

(Continued)

Table 2 (continued)

	Author	Type of IDS	Level 1	Level 2	Level 3
17	Neupane et al., 2022 [39]	Explainable-IDS	White Box	Regression	
				Rule-Based	
				Statistical & Probabilistic	
				Clustering	
			Black Box	Feature	
				Perturbation	
				Decomposition	
				Hybrid	
18	Spadaccino and Cuomo, 2022 [7]	IDS for IoT Devices	Devices	Cloud Servers	
				Edge Devices	
				Gateway	
				End Devices	
			Access Technology	BLE	
				Wi-Fi	
				LoRaWAN	
				Cellular-like	
			Adopted Technique	Signature-based	
				Anomaly-based	
				Specification-based	
			Computing Architecture	Centralized	
				Hybrid-Clustred	
				Fully distributed	
			Performance Objectives	Energy saving	
				Latency	
				Execution time	
				Data Reduction	

(Continued)

Table 2 (continued)

	Author	Type of IDS	Level 1	Level 2	Level 3
19	Santhosh Kumar et al., 2023 [40]	IDS in IoT	Based on Intrusion detection mechanism	IDS based on Anomaly	
				IDS based on Signature	
				IDS based on Specification	
				Hybrid IDS	
			Detection Based on network structure	Centralized IDS	
				Distributed IDS	
				Hybrid IDS	
			Detection based on attacks	Denial of Service Attack	
				Replay attack	
				Sybil attack	
				Wormhole attack	
				False data attack	
				Jamming attack	
20	Liao et al., 2024 [41]	IDS in IoT	Technology Based	Anomaly detection	
				Misuse detection	
			Data source based	Host based	
				Network based	
21	Khalid and Aldabagh, 2024 [42]	IDS in SDN	Types	HIDS	
				NIDS	
			Detection method	Signature based	
				Anomaly based	
				Hybrid	
			Inspection method	Flow based	
				Packet based	
			Deployment	Centralized	
				Distributed	

(Continued)

Table 2 (continued)

	Author	Type of IDS	Level 1	Level 2	Level 3
22	He et al., 2024 [43]	Approaches to Energy-Aware Security	Hardware based Approaches	(1) Low-power processors (2) Energy-efficient communication modules (3) Cryptographically secure enclaves	
			Software based Approaches	(1) Lightweight cryptographic algorithms (2) Optimized security protcols (3) Contex-based adaptive security level	
			Network based Approaches	(1) Energy-eficient Communication Protocols (2) Network Segmentation (3) Collaborative Security Between Devices	
			Data centric Approaches	(1) Data Aggregation and Compression (2) In-network processing	
			Machine Learning Methods	(1) Anomaly Detection and Intrusion Prevention (2) Real-time monitoring	
23	Satilmis et al., 2025 [44]	IDSs	Data Source	Network based	
				Host based	
			Detection Method	Signature based	
				Anomaly based	
			Response/Reaction	Passive	
				Active	

Table 3 summarizes the frequency of IDS approaches employed across the reviewed studies. The most prevalent detection paradigms are anomaly-based, misuse-based (signature-based), host-based, network-based, and hybrid IDSs, which collectively represent the dominant strategies in cybersecurity intrusion detection. These approaches are widely adopted across IT, IoT, and IIoT environments, reflecting their broad applicability and adaptability. Notably, distributed architectures emerge as the preferred deployment strategy for IoT and IIoT systems, owing to their scalability and resilience in resource-constrained, heterogeneous networks. In contrast, specialized techniques, such as hierarchical energy-efficient designs or control-process analysis-based, methods appear only in niche studies tailored to specific system requirements. This distribution underscores a critical gap: emerging threats such as adversarial attacks remain underexplored in prior taxonomies, highlighting the need for more comprehensive classification frameworks.

Table 3: Frequency of different approaches in reviewed papers.

	Approaches	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Total Papers
1	Host Based	v			v	v		v	v		v	v	v				v			v		v	v		13
2	Network Based	v			v	v		v	v		v	v	v				v			v		v	v		13
3	Anomaly Detection	v	v	v				v	v	v	v	v	v	v		v	v	v		v	v	v	v		18
4	Misuse Detection	v	v	v				v	v			v	v	v		v	v	v			v	v	v		15
5	Active	v																						v	2
6	Passive	v																						v	2
7	Distributed		v	v	v	v			v		v			v			v				v		v		10
8	Centralized			v					v					v				v			v		v		6
9	Decentralized								v																1
10	Hierarchical Energy Efficient Based		v																						1
11	Cluster-Based		v																						1
12	Hypothetical			v										v											2
13	Empirical			v										v											2
14	Simulation			v										v											2
15	Theoretical			v										v											2
16	Hybrid Based		v	v	v	v			v							v	v				v		v		9
17	Protocol Based						v																		1
18	Database IDS					v																			1
19	Hypervisor Based					v										v									2
20	traffic mining based						v																		1
21	control process analysis-based						v																		1
22	Tracing and debugging embedded device									v															1
23	Security Methods and Attacks			v							v										v				3
24	Customized IDS																v								1
25	Devices																	v							1
26	Access Technology																	v							1
27	Specification			v				v										v			v				4
28	Latency																	v							1
29	Execution Time																	v							1
30	Data Reduction																	v							1
31	White Box																		v						1
32	Black Box																		v						1
33	Virtualization															v									1
34	Automatic response												v												1
35	Notification Only												v												1
36	Cyber Threats																								1
37	Cybersecurity issues																								1
38	Flow Based																						v		1
39	Packet based																						v		1
40	Hardware based																							v	1
41	Software based																							v	1
42	Network based																							v	1
43	Data centric																							v	1
44	Machine Learning Methods																							v	1

Note: v = signifies the presence of the approach in the paper corresponding to its index in Table 2.

To facilitate quantitative comparison, numeric codes were assigned to each IDS technique analyzed in this study. Fig. 3 visualizes the frequency of each approach across the reviewed literature, with the accompanying pie chart illustrating the proportional usage of each technique in designed IDS architectures. Anomaly-based (18%), signature-based (15%), host-based (13%), and network-based (13%) methods constitute the most frequently discussed paradigms in both IT and OT contexts. Distributed (9%) and centralized (5%) architectures follow, while remaining approaches are typically oriented toward specialized applications, particularly in IoT platforms. It is important to note that IDS design is inherently linked to the

underlying detection methodology, which in turn determines how effectively the system can identify and mitigate vulnerabilities exploited by specific attack vectors. Consequently, while certain techniques—such as anomaly-based detection—are broadly applicable, others are deployed only in targeted research contexts. Furthermore, critical methodologies such as binary and multiclass classification, as well as emerging threat categories like adversarial machine learning attacks, are not traditionally categorized as standalone IDS approaches in prior literature. Their omission from conventional taxonomies motivates the development of a more nuanced and forward-looking classification framework for IDS research.

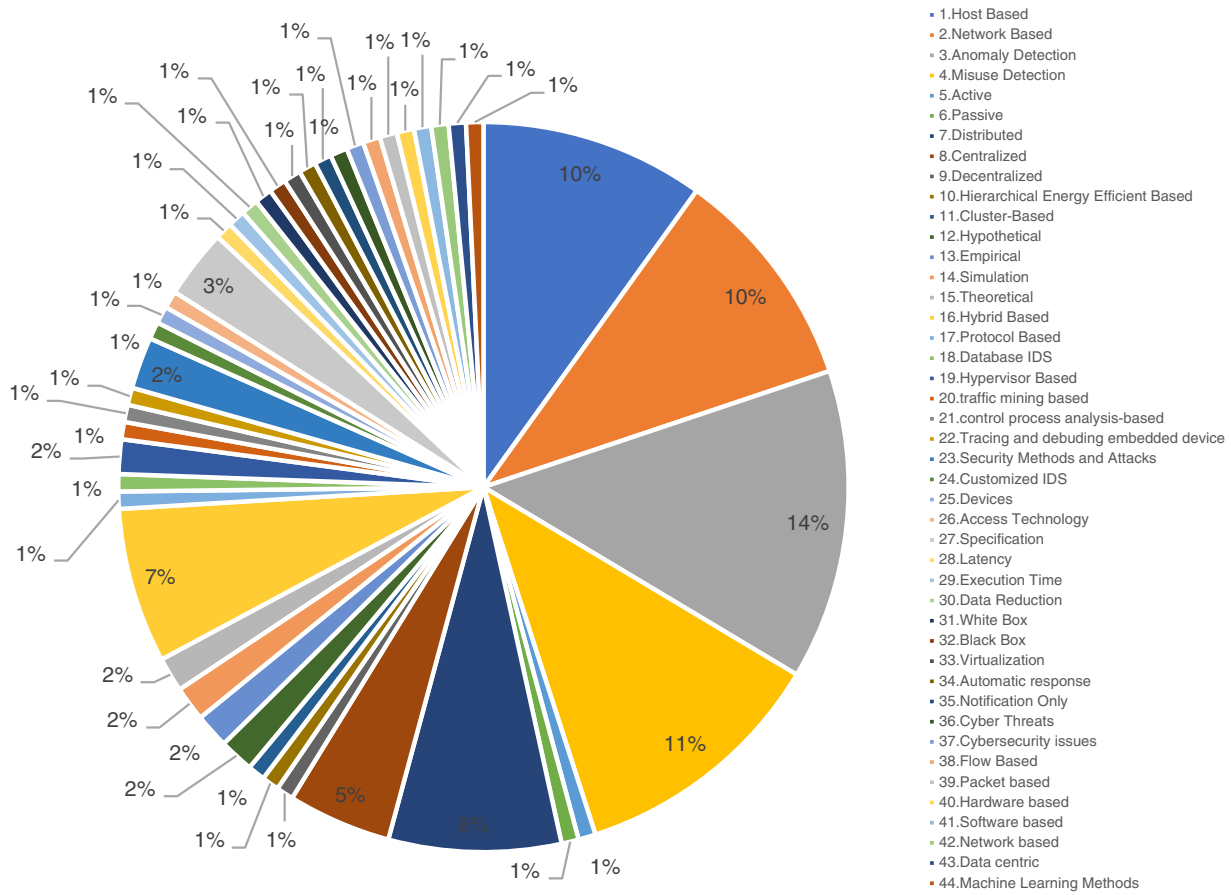

Figure 3: Pie chart of different approach frequencies.

5 Taxonomy of IDS for IIoT

The rapid evolution of industrial technologies continuously introduces novel vulnerabilities alongside increasingly sophisticated cyber threats. In this dynamic landscape, the development of adaptive cybersecurity strategies is indispensable, particularly for intrusion detection systems (IDS). To effectively mitigate the escalating risks targeting critical infrastructure (CI), a comprehensive and context-aware taxonomy is required. As noted in [45], IDS architectures must be tailored to the specific characteristics of the underlying network, as attack vectors are inherently tied to network topology and operational constraints. Consequently, threats must be systematically categorized by their properties, behaviors, and attack methodologies. A well-structured taxonomy enables security practitioners to accurately distinguish anomalies, streamline threat response, and enhance overall IDS efficacy.

Existing surveys and taxonomies for IT and IoT environments typically classify IDS by deployment location (host vs. network), detection methodology (signature, anomaly, specification, hybrid), and validation strategy. While these frameworks provide valuable baselines and confirm the growing dominance of ML/DL-driven anomaly detection, they exhibit three critical limitations when applied to IIoT contexts: (i) Most classifications treat deployment at a high level (e.g., host vs. network, centralized vs. distributed) without explicitly mapping these categories to IIoT architectural segmentation (e.g., IT/OT separation, industrial DMZs) or OT-specific operational requirements such as availability and physical safety. This gap hinders practical deployment planning in real industrial environments. (ii) As IDS increasingly rely on ML/DL models, as demonstrated in CI-focused works [12] and federated learning approaches [19,46], threat models must account for adversarial manipulation and data/model poisoning. Yet, adversarial robustness is rarely treated as a first-class dimension in existing taxonomies. (iii) Many surveys offer descriptive overviews but lack practitioner-facing mappings between IDS categories and engineering constraints (e.g., online vs. offline operation, OT-appropriate response behaviors, and the implications of binary vs. multiclass outputs). To address these gaps, the proposed taxonomy introduces an Infrastructure Domain dimension that differentiates IIoT subfields with distinct operational constraints. For instance, the Internet of Medical Things (IoMT) emphasizes privacy and regulatory compliance, favoring host-based monitoring and privacy-preserving techniques. Conversely, the Internet of Vehicles (IoV) prioritizes mobility, low latency, and intermittent connectivity, making distributed NIDS and real-time detection more suitable. By explicitly classifying IDS across domains, deployment architecture, and operational mode, this taxonomy enables the selection of feasible, context-aware IDS solutions aligned with each subfield's resource, latency, and safety requirements.

Illustrative Example: Consider an edge-assisted IDS deployed in a smart manufacturing facility. Traffic is mirrored at OT gateways and programmable logic controllers (PLCs), functioning as a network-based IDS (NIDS) [47]. Gateways positioned at the network edge monitor inbound and outbound communications from field devices, while sensors report to decentralized monitoring nodes. Detection employs a hybrid LSTM-based anomaly model augmented with signature matching for known malware. The system operates in real-time (online mode), outputs multiclass attack labels, targets IIoT/OT layers, and incorporates adversarial training to mitigate evasion techniques. This example demonstrates how the proposed taxonomy facilitates the precise specification, comparison, and deployment of industrial IDS architectures.

The primary value of this taxonomy lies in its ability to reduce implementation complexity and operational overhead by aligning cybersecurity controls with actual threat profiles rather than relying on generic, one-size-fits-all frameworks. Security architects can leverage this classification to select optimal IDS configurations, ensuring more efficient resource allocation and stronger defense postures. Furthermore, the taxonomy establishes standardized terminology that improves communication among stakeholders, management, and engineering teams, bridging the gap between high-level cybersecurity policies and practical implementation.

Accordingly, this section presents a novel taxonomy designed to address the limitations identified in prior literature. Fig. 4 illustrates the proposed classification framework for IIoT environments.

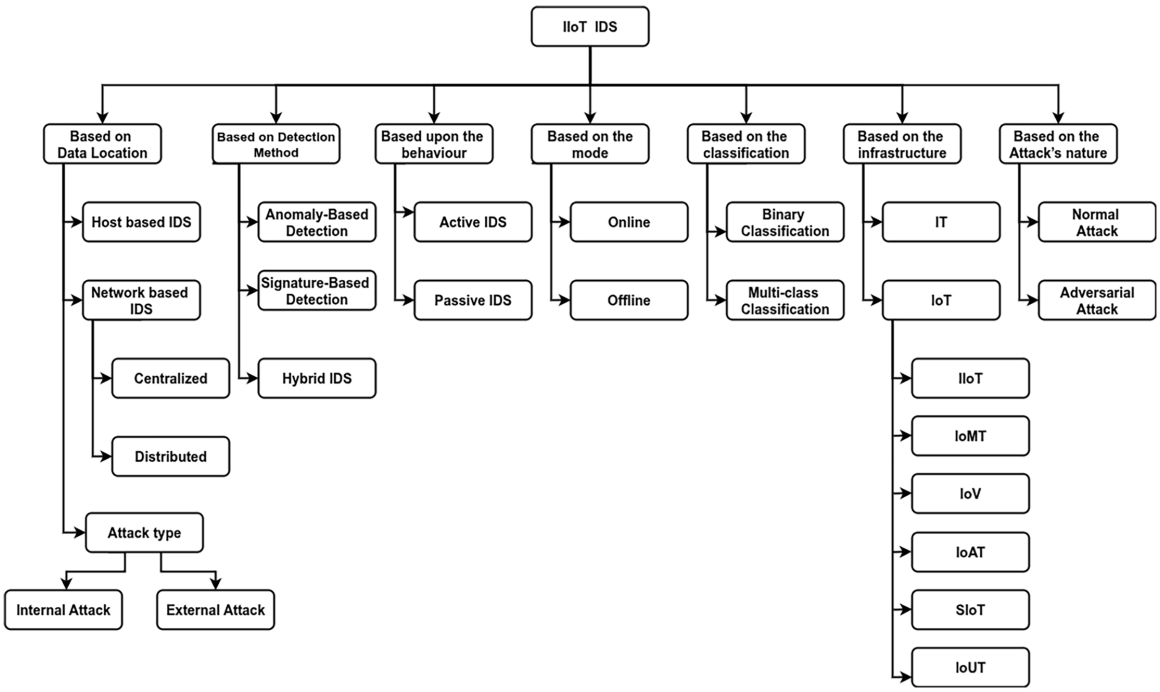

Figure 4: Taxonomy of IDS in IIoT.

5.1 Based on Data Location

This IDS is based on the type of attack depending on its placement in the infrastructure. It is considered a cybersecurity tool that operates on particular nodes of the Network as Host-based or on the entire network qualified as a Network-based IDS.

5.1.1 Host-Based IDS (HIDS)

Deployed on individual endpoints, HIDS monitors system logs, file integrity, process behavior, and user activities on servers, workstations, or PLC-adjacent hosts. It provides granular, host-level visibility but does not monitor cross-node network traffic.

5.1.2 Network-Based IDS (NIDS)

Deployed at strategic points within the network topology, NIDS inspects packet flows and protocol traffic to detect threats across the infrastructure. While it offers broad visibility, it may generate higher false-positive rates, particularly under encrypted or high-throughput conditions. NIDS architectures are further categorized by deployment topology, as illustrated in Fig. 5.

Centralized IDS: Operates on a star-like architecture where distributed sensors forward traffic data to a central analysis unit. This model aligns with IoT systems that rely on centralized data storage [48]. The central node, typically deployed at edge routers or dedicated analysis hosts [8], applies security rules to detect threats and coordinate mitigation responses [49].

Distributed IDS: Comprises multiple autonomous nodes that independently analyze traffic and exchange threat intelligence across heterogeneous networks [15]. This architecture enables detection at any network endpoint and evenly distributes computational loads, allowing each monitoring point to classify traffic locally [50].

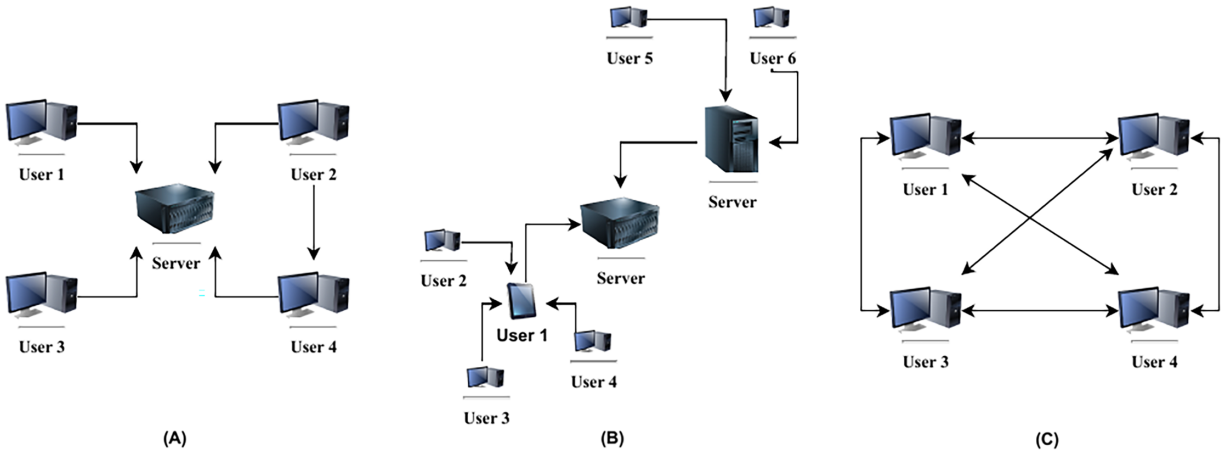

Figure 5: Architecture of NIDS: (**A**) Centralized, (**B**) Decentralized, and (**C**) Distributed.

Decentralized IDS: Organizes sensors into localized clusters managed by regional coordinators, which aggregate and relay data to a central authority. Monitoring can follow a hierarchical ranking or operate via autonomous, peer-to-peer IDS nodes [50].

5.1.3 Attack Type

An IDS is considered a tool developed to block suspected threats. However, the vast expansion of modern infrastructure has led to various attacks. Indeed, with more evolution and diversification of the network, more vulnerabilities are encountered, attackers are sophisticated, and cyberattacks are miscellaneous.

The attackers used two types of attacks: internal and external, as shown in Fig. 6. Internal attacks are carried out by a user or intruder within the infrastructure, making intrusion easier. However, external attacks are manipulated from outside the network, making them more complex.

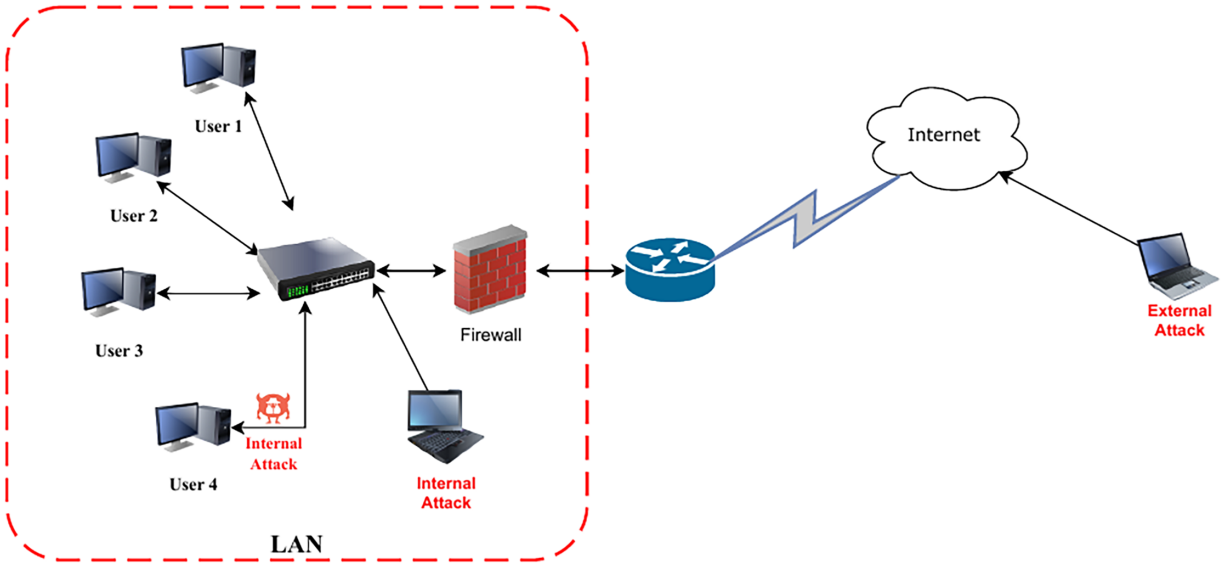

Figure 6: Representation of internal and external attacks.

Ref. [51], the IDS within a network is subject to internal attacks because an attacker from the infrastructure can reach it and launch attacks. As noted in [35], combining NIDS with HIDS and firewalls provides layered defense against both internal and external threats [37]. HIDS monitors the network for abnormal behavior. Meanwhile, the NIDS scans the entire infrastructure for internal and external networks.

5.2 Based on Detection Methods

This dimension categorizes IDS by the underlying mechanism used to identify malicious activity. Anomaly-based and signature-based methods are the two most popular detection methods [52].

5.2.1 Anomaly-Based Detection (AIDS)

Anomalous behavior is used to detect threats. The IDS studies network traffic and checks for abnormal activities. The development of IIoT raises cyberattacks and their variation within industries, thereby lowering anomaly detection. Therefore, the progress in anomaly detection should improve information handling and security [53]. Indeed, the new trend in anomaly detection uses machine learning (ML) algorithms to enhance detection.

ML is more proficient in distinguishing anomalies than regular users. The precious characteristic of ML to learn and progress makes it prominent in view of the fact that attacks are permanently growing and unknown vulnerabilities are frequently located [54].

5.2.2 Signature-Based Detection (SIDS)

This technique focuses on the attack pattern and verifies the existence of its signature in previously prepared databases. Indeed, every known malware or attack is recorded as a reference for review during the checking phase. This approach is efficient against known attacks. However, it could be more efficient for zero-day attacks [55].

5.2.3 Hybrid IDS

This type of IDS combines both anomaly- and signature-based detection methods. This benefits both the techniques [37]. SIDS is rapid and easy to build, and AIDS can discover new threats. Hence, each method has specific weaknesses. Thus, a hybrid IDS is associated with different IDS techniques that establish a protected solid network.

5.3 Based upon the Behavior

This type of IDS is not based on network flow behavior; it is principally related to the behavior of the IDS itself. It can be an active or passive IDS.

The most well-known IDSs are built as passive reactions against threats, and passive reaction systems only alert the administrator and log attack information without any action against the attack itself. However, active systems attempt to find an attacker or even cause damage to mitigate the offense [56].

5.3.1 Active IDS

Logs the attacks to prevent, block, or mitigate attacks. Thus, they play the role of detection and prevention, from which we often find intrusion detection and prevention systems (IDPS). It is considered a shield and a real-time defender.

5.3.2 Passive IDS

It only detects and analyzes the network and logs the activities of the expected attacks. It does not protect the network by blocking malicious activities; it monitors and reports to the central unit.

5.4 Based on the Mode

In this IDS, the operation is based on the time spent monitoring network traffic, either offline, through datasets collected from previous traffic or in real-time traffic [57]. Reported that this IDS is based on usage frequency, and it is principally the time passed from the data collection and the analysis of the traffic recorded.

5.4.1 Online

This type of IDS is connected to the network, and simultaneously monitors and tracks threats in the flow. It is real-time monitoring of the network, which means the actual detection of the threats and standing against the attacks before the strike.

5.4.2 Offline

In this method, the network flow is a packet in datasets, and at a later time, the analysis is processed by the IDS. Ref. [57] Due to the big data circling in IoT devices, this type of detection is preferable. Offline IDS is not an accurate time detection. However, it offers deep training in the IDS model, making it more robust against attacks.

5.5 Based on the Classification

Primary IDS research provides outputs based on the classification of the samples in the dataset. However, there are two types of classification: binary and multiclass. The importance of both techniques requires integration into intrusion strategies.

5.5.1 Binary Classification

Data were classified as either normal or malicious. Accordingly, specific studies used binary classification to organize the data into two categories: attack or benign.

It is faster to train and requires fewer computational resources than other methods. However, it is restricted to bi-classes and misses the attack details.

5.5.2 Multi-Class Classification

This type of IDS detects normal traffic, and malicious traffic is classified into multiple categories depending on the number of classes to detect benign traffic and attacks in the dataset. Thus, it provided more precise information. However, the process is complex. In addition, other research developed an IDS that classifies data using both techniques; for example, [58] evaluates binary and multiclass models across four IoT datasets, while [59] applies both classifications and uses the NSL-KDD dataset.

5.6 Based on the Infrastructure

5.6.1 IT

Presents the most well-known IDSs that audit data in typical computer networks. The main task of the infrastructure is to protect the workstations, printers, servers, and common network nodes. This type of IDS has been intensely investigated for years, owing to the need for security inside IT platforms.

5.6.2 IoT

In this category, the new network technologies use sensors, controllers, and edge devices. Thus, the information gathered differs from that in IT, implying that new vulnerabilities and attacks exist. Hence, an IDS must overcome the IT and IoT threats. The expansion of IoT platforms across diverse fields has recently drawn increased attention from cybersecurity researchers. Yet, the heterogeneity of IoT components and the scalability of the underlying infrastructure continue to complicate cyber protection efforts. This has led to the emergence of distinct IoT variants tailored to specific application domains [60]. Among them are industrial IoT (IIoT), applications in healthcare (IoMT), transportation (IoV), farming (Internet of Agriculture Things—IoAT), and Social Internet of Things (SIoT). Add to that the Internet of Underwater Things (IoUT).

IIoT: Here, we determine the total traffic flow configuration, consisting of standard networks and industrial traffic within the same infrastructure. IIoT systems process complex tasks and a significant amount of data, which means they require increased protection. The widespread adoption of IoT in industrial settings, coupled with the increasing use of wireless technologies, has transformed industrial automation and control systems (IACS), giving rise to the Industrial Internet of Things (IIoT) and eliminating the isolation traditionally associated with ICT infrastructures [61]. Consequently, IDSs have been introduced in IIoT platforms to secure these systems.

IoMT: The Internet of Medical Things (IoMT) presents the application of IoT in the medical field [62]. The Internet of Things has modified the healthcare sector by introducing the IoMT.

IoV: The Internet of Vehicles (IoV) denotes a large-scale distributed system that could be seen as the convergence of the mobile Internet and the Internet of Things (IoT) [63]. IoV represents an evolution of vehicular communication networks, moving beyond the traditional Vehicular *Ad hoc* Network (VANET) toward a more sophisticated framework that enables dynamic interactions among vehicles, traffic management systems, and other domain-specific entities.

IoAT: Discussed the use of Internet of Agro Things (IoAT) in farming. IoAT increases the efficiency of farm administration and resource management, makes farm operations economically viable, improves harvest yields, and enhances environmental monitoring and surveillance [64].

SIoT: The Social Internet of Things (SIoT) refers to the socialization of IoT, in which devices establish social connections [65]. SIoT is fundamentally transforming our daily interactions and can radically alter how we engage with smart devices by introducing a social component to connected devices [66].

IoUT: Federated Learning (FL) has been adopted to strengthen data security and intrusion detection capabilities within Internet of Underwater Things (IoUT) environments [67].

5.7 Based on the Attack's Nature

With the apparition of artificial intelligence, the attacks are divided into two categories: normal and adversarial. Normal attacks involve directly manipulating the input data to cause misclassification. This kind of attack is easily detectable by a well-trained IDS. However, adversarial attacks that are generated from noise are hard to detect.

5.7.1 Normal Attacks

Follow established attack patterns (e.g., DoS, port scanning, malware execution). These are well-documented and effectively detected by mature IDS frameworks across IT, IoT, and IIoT environments. They can cause data exfiltration, system disruption, or unauthorized control of critical processes.

5.7.2 Adversarial Attacks (Adv. Attks.)

This type of IDS detects attacks designed to evade detection. Evasion is possible by creating attacks that mimic normal traffic behavior. The susceptibility of ML to adversarial attacks is a significant factor contributing to its exposure to threats [68]. Thus, it is necessary to develop robust machine learning models to mitigate insider threats. A robust model is an ML algorithm capable of resisting adversarial attacks. Furthermore, various devices within the IIoT infrastructure generate information across different dimensions. The data collected from the domain of study determines the nature of the adversarial attack generation method [12]. Thus, the Adv. Attks. It is crucial in IDS studies because of the continual improvement in these intelligent attacks.

6 Conclusion and Future Work

This paper reviewed intrusion detection systems (IDS) across IT, IoT, and IIoT/ICS environments to identify limitations in existing IDS classifications for industrial deployments. Recent research favors anomaly-based detection, often powred by ML/DL, while exploring distributed architectures, explainability, and privacy-aware learning for large scale, segmented IIoT infrastructures. Yet adversarial machine learning remains underexplored, despite its rising relevance.

This analysis synthesizes IDS trends in IT, IoT, and IIoT/ICS, revealing how IIoT constraints such as heterogeneity, segmentation, and OT safety requirements shape design choices.

A methodical comparison of representative IDS approaches has been provided, pinpointing trends and gaps. Building on this, an IIoT-oriented taxonomy is proposed to consolidate the key dimensions: data source and deployment, detection method, behavior and mode, output granularity, infrastructure scope, and explicitly incorporates attack nature, including overlooked adversarial threats.

Future research should prioritize deployability and robustness in real industrial settings over taxonomy design alone. Key directions include:

- Evaluate taxonomy-driven IDS designs using real industrial traffic, process telemetry, and public ICS datasets, with performance reported under class imbalance and concept drift.
- Systematically testing ML/DL-based IDS against adversarial threats and benchmark defenses such as adversarial training.
- Developing resource-efficient IDS for PLC-adjacent devices, gateways, and edge nodes, optimizing memory, latency, and energy while sustaining detection accuracy.

Addressing these directions will strengthen the practical impact of IDS research and support the dvelopment of robust, scalable, and operationally safe detection solutions for IIoT infrastructures.

Acknowledgement: Not applicable.

Funding Statement: This research is supported in part by the Ministry of Higher Education—the University Kebangsaan Malaysia, Malaysia, through Fundamental Research Grant Scheme (FRGS/1/2023/ICT07/UKM/02/3).

Author Contributions: Conceptualization: Ali Lamjid. Formal Analysis: Ali Lamjid, Khairul Akram Zainol Ariffin. Supervision: Khairul Akram Zainol Ariffin, Mohd Juzaiddin Ab Aziz, Nor Samsiah Sani. Project Administration: Ali Lamjid. Writing—Original Draft: Ali Lamjid. Writing—Review & Editing: Ali Lamjid, Khairul Akram Zainol Ariffin. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: This article does not involve data availability, and this section is not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

CNN	Convolutional Neural Network
DL	Deep Learning
DNS	Domain Name System
DoS	Denial of Service
HMI	Human Machine Interface
LSTM	Long Short Term Memory
MiTM	Man in The Middle
ML	Machine Learning
PLC	Programmable Logic Controller
RNN	Recurrent Neural Network
SVM	Support Vector Machine

References

1. Elrawy MF, Awad AI, Hamed HFA. Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comput. 2018;7(1):21. doi:10.1186/s13677-018-0123-6.
2. Hu Y, Yang A, Li H, Sun Y, Sun L. A survey of intrusion detection on industrial control systems. Int J Distrib Sens Netw. 2018;14(8):155014771879461. doi:10.1177/1550147718794615.
3. Ahmad Z, Shahid Khan A, Wai Shiang C, Abdullah J, Ahmad F. Network intrusion detection system: a systematic study of machine learning and deep learning approaches. Trans Emerg Telecommun Technol. 2021;32(1):e4150. doi:10.1002/ett.4150.
4. Sattarpour S, Barati A, Barati H. EBIDS: efficient BERT-based intrusion detection system in the network and application layers of IoT. Clust Comput. 2024;28(2):138. doi:10.1007/s10586-024-04775-y.
5. Dini P, Elhanashi A, Begni A, Saponara S, Zheng Q, Gasmi K. Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity. Appl Sci. 2023;13(13):7507. doi:10.3390/app13137507.
6. Hossain MA, Islam MS. Ensuring network security with a robust intrusion detection system using ensemble-based machine learning. Array. 2023;19(2):100306. doi:10.1016/j.array.2023.100306.
7. Spadaccino P, Cuomo F. Intrusion detection systems for IoT: opportunities and challenges offered by edge computing. ITU J Future Evol Technol. 2022;3(2):408–20. doi:10.52953/wnvi5792.
8. Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC. A survey of intrusion detection in Internet of Things. J Netw Comput Appl. 2017;84(3):25–37. doi:10.1016/j.jnca.2017.02.009.
9. Ungurean I, Gaitan NC. A software architecture for the industrial Internet of Things-a conceptual model. Sensors. 2020;20(19):5603. doi:10.3390/s20195603.
10. Ullah I, Mahmoud QH. Design and development of RNN anomaly detection model for IoT networks. IEEE Access. 2022;10:62722–50. doi:10.1109/ACCESS.2022.3176317.
11. Li J, Liu Y, Chen T, Xiao Z, Li Z, Wang J. Adversarial attacks and defenses on cyber–physical systems: a survey. IEEE Internet Things J. 2020;7(6):5103–15. doi:10.1109/JIOT.2020.2975654.
12. Khazane H, Ridouani M, Salahdine F, Kaabouch N. A holistic review of machine learning adversarial attacks in IoT networks. Future Internet. 2024;16(1):32. doi:10.3390/fi16010032.
13. Hindistan S, Yetkin EF. A hybrid approach with GAN and DP for privacy preservation of IIoT data. IEEE Access. 2023;11(1):5837–49. doi:10.1109/access.2023.3235969.
14. Cherbal S, Zier A, Hebal S, Louail L, Annane B. Security in Internet of Things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. J Supercomput. 2024;80(3):3738–816. doi:10.1007/s11227-023-05616-2.
15. Panchal AC, Khadse VM, Mahalle PN. Security issues in IIoT: a comprehensive survey of attacks on IIoT and its countermeasures. In: Proceedings of the 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN); 2018 Nov 23–24; Lonavala, India. p. 124–30. doi:10.1109/GCWCN.2018.8668630.

16. Mekala SH, Baig Z, Anwar A, Zeadally S. Cybersecurity for Industrial IoT (IIoT): threats, countermeasures, challenges and future directions. Comput Commun. 2023;208:294–320. doi:10.1016/j.comcom.2023.06.020.
17. Binnar P, Bhirud S, Kazi F. Security analysis of cyber physical system using digital forensic incident response. Cyber Secur Appl. 2024;2(5):100034. doi:10.1016/j.csa.2023.100034.
18. Radoglou-Grammatikis P, Sarigiannidis P, Iturbe E, Rios E, Sarigiannidis A, Nikolis O, et al. Secure and private smart grid: the SPEAR architecture. In: Proceedings of the 2020 6th IEEE Conference on Network Softwarization (NetSoft); 2020 Jun 29–Jul 3; Ghent, Belgium.
19. Radoglou-Grammatikis P, Liatifis A, Dalamagkas C, Lekidis A, Voulgaridis K, Lagkas T, et al. ELECTRON: an architectural framework for securing the smart electrical grid with federated detection, dynamic risk assessment and self-healing. In: Proceedings of the 18th International Conference on Availability, Reliability and Security; 2023 Aug 29–Sep 1; Benevento, Italy. doi:10.1145/3600160.3605161.
20. Suaboot J, Fahad A, Tari Z, Grundy J, Mahmood AN, Almalawi A, et al. A taxonomy of supervised learning for IDSs in SCADA environments. ACM Comput Surv. 2021;53(2):1–37. doi:10.1145/3379499.
21. Sun D, Hu J, Wu H, Wu J, Yang J, Sheng QZ, et al. A comprehensive survey on collaborative data-access enablers in the IIoT. ACM Comput Surv. 2024;56(2):1–37. doi:10.1145/3612918.
22. Srivastava A, Gupta S, Quamara M, Chaudhary P, Aski VJ. Future IoT-enabled threats and vulnerabilities: state of the art, challenges, and future prospects. Int J Commun Syst. 2020;33(12):e4443. doi:10.1002/dac.4443.
23. Shah Y, Sengupta S. A survey on classification of cyber-attacks on IoT and IIoT devices. In: Proceedings of the 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON); 2020 Oct 28–31; New York, NY, USA. doi:10.1109/uemcon51285.2020.9298138.
24. Sherasiya T, Upadhyay H, Patel HB. A survey: intrusion detection system for internet of things. Int J Comput Sci Eng. 2016;5(2):91–8.
25. Anwar S, Mohamad Zain J, Zolkipli MF, Inayat Z, Khan S, Anthony B, et al. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms. 2017;10(2):39. doi:10.3390/a10020039.
26. Othman SM, Alsohybe NT, Ba-Alwi FM, Zahary AT. Survey on intrusion detection system types. Int J Cyber-Secur Digit Forensics. 2018;7(4):444–63.
27. Nisioti A, Mylonas A, Yoo PD, Katos V. From intrusion detection to attacker attribution: a comprehensive survey of unsupervised methods. IEEE Commun Surv Tutor. 2018;20(4):3369–88. doi:10.1109/COMST.2018.2854724.
28. Gassais R, Ezzati-Jivan N, Fernandez JM, Aloise D, Dagenais MR. Multi-level host-based intrusion detection system for Internet of Things. J Cloud Comput. 2020;9(1):62. doi:10.1186/s13677-020-00206-6.
29. Tsiknas K, Taketzis D, Demertzis K, Skianis C. Cyber threats to industrial IoT: a survey on attacks and countermeasures. IoT. 2021;2(1):163–86. doi:10.3390/iot2010009.
30. Biggio B, Roli F. Wild patterns: ten years after the rise of adversarial machine learning. Pattern Recognit. 2018;84(3):317–31. doi:10.1016/j.patcog.2018.07.023.
31. Chen F, Luo D, Xiang T, Chen P, Fan J, Truong HL. IoT cloud security review: a case study approach using emerging consumer-oriented applications. ACM Comput Surv. 2022;54(4):1–36. doi:10.1145/3447625.
32. Lazrek G, Chetioui K, Balboul Y, Mazer S, bekkali El M. An RFE/Ridge-ML/DL based anomaly intrusion detection approach for securing IoMT system. Results Eng. 2024;23(24):102659. doi:10.1016/j.rineng.2024.102659.
33. Acharya N, Singh S. An analysis of feature selection based design methods of IDS. Int J Comput Sci Inf Secur. 2016;14(8):558.
34. Sicato JCS, Singh SK, Rathore S, Park JH. A comprehensive analyses of intrusion detection system for IoT environment. J Inf Process Syst. 2020;16(4):975–90. doi:10.3745/JIPS.03.0144.
35. Khraisat A, Alazab A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity. 2021;4(1):18. doi:10.1186/s42400-021-00077-7.
36. Dhirani LL, Armstrong E, Newe T. Industrial IoT, cyber threats, and standards landscape: evaluation and roadmap. Sensors. 2021;21(11):3901. doi:10.3390/s21113901.

37. Lata S, Singh D. Intrusion detection system in cloud environment: literature survey & future research directions. Int J Inf Manag Data Insights. 2022;2(2):100134. doi:10.1016/j.jjimei.2022.100134.
38. Khan AR, Kashif M, Jhaveri RH, Raut R, Saba T, Ali Bahaj S. Deep learning for intrusion detection and security of Internet of Things (IoT): current analysis, challenges, and possible solutions. Secur Commun Netw. 2022;2022(4):4016073. doi:10.1155/2022/4016073.
39. Neupane S, Ables J, Anderson W, Mittal S, Rahimi S, Banicescu I, et al. Explainable intrusion detection systems (X-IDS): a survey of current methods, challenges, and opportunities. IEEE Access. 2022;10(7):112392–415. doi:10.1109/ACCESS.2022.3216617.
40. Santhosh Kumar SVN, Selvi M, Kannan A. A comprehensive survey on machine learning-based intrusion detection systems for secure communication in Internet of Things. Comput Intell Neurosci. 2023;2023(1):8981988. doi:10.1155/2023/8981988.
41. Liao H, Murah MZ, Hasan MK, Aman AHM, Fang J, Hu X, et al. A survey of deep learning technologies for intrusion detection in Internet of Things. IEEE Access. 2024;12(1):4745–61. doi:10.1109/ACCESS.2023.3349287.
42. Khalid HYI, Aldabagh NBI. A survey on the latest intrusion detection datasets for software defined networking environments. Eng Technol Appl Sci Res. 2024;14(2):13190–200. doi:10.48084/etasr.6756.
43. He P, Zhou Y, Qin X. A survey on energy-aware security mechanisms for the Internet of Things. Future Internet. 2024;16(4):128. doi:10.3390/fi16040128.
44. Satilmiş H, Akleylek S, Tok ZY. A systematic literature review on host-based intrusion detection systems. IEEE Access. 2024;12(1):27237–66. doi:10.1109/ACCESS.2024.3367004.
45. Alkasassbeh M, Al-Haj Baddar S. Intrusion detection systems: a state-of-the-art taxonomy and survey. Arab J Sci Eng. 2023;48(8):10021–64. doi:10.1007/s13369-022-07412-1.
46. Bukhari SMS, Zafar MH, Abou Houran M, Qadir Z, Kumayl Raza Moosavi S, Sanfilippo F. Enhancing cybersecurity in Edge IIoT networks: an asynchronous federated learning approach with a deep hybrid detection model. Internet Things. 2024;27(4):101252. doi:10.1016/j.iot.2024.101252.
47. Shojarazavi T, Barati H, Barati A. A wrapper method based on a modified two-step league championship algorithm for detecting botnets in IoT environments. Computing. 2022;104(8):1753–74. doi:10.1007/s00607-022-01070-9.
48. Kumar R, Kumar P, Tripathi R, Gupta GP, Garg S, Hassan MM. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. J Parallel Distrib Comput. 2022;164(2):55–68. doi:10.1016/j.jpdc.2022.01.030.
49. Segura GAN, Chorti A, Margi CB. Centralized and distributed intrusion detection for resource-constrained wireless SDN networks. IEEE Internet Things J. 2022;9(10):7746–58. doi:10.1109/JIOT.2021.3114270.
50. Vasilomanolakis E, Karuppayah S, Mühlhäuser M, Fischer M. Taxonomy and survey of collaborative intrusion detection. ACM Comput Surv. 2015;47(4):1–33. doi:10.1145/2716260.
51. Ahmad A, Zainudin WS, Kama MN, Idris NB, Mohd Saudi M, Zakaria NH. State of the art intrusion detection system for cloud computing. Int J Commun Netw Inf Secur. 2018;10(3):480. doi:10.17762/ijcnis.v10i3.3590.
52. Ali F, El-Sappagh S, Riazul Islam SM, Kwak D, Ali A, Imran M, et al. A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion. Inf Fusion. 2020;63:208–22. doi:10.1016/j.inffus.2020.06.008.
53. Bakhsh SA, Khan MA, Ahmed F, Alshehri MS, Ali H, Ahmad J. Enhancing IoT network security through deep learning-powered Intrusion Detection System. Internet Things. 2023;24:100936. doi:10.1016/j.iot.2023.100936.
54. Zolanvari M, Teixeira MA, Gupta L, Khan KM, Jain R. Machine learning-based network vulnerability analysis of industrial Internet of Things. IEEE Internet Things J. 2019;6(4):6822–34. doi:10.1109/jiot.2019.2912022.
55. Al-Asiri M, El-Alfy EM. On using physical based intrusion detection in SCADA systems. Procedia Comput Sci. 2020;170:34–42. doi:10.1016/j.procs.2020.03.007.
56. Stakhanova N, Basu S, Wong J. A taxonomy of intrusion response systems. Int J Inf Comput Secur. 2007;1(1/2):169. doi:10.1504/ijics.2007.012248.
57. Kamaldeep, Dutta M, Granjal J. Towards a secure internet of things: a comprehensive study of second line defense mechanisms. IEEE Access. 2020;8:127272–312. doi:10.1109/ACCESS.2020.3005643.

58. Fraihat S, Makhadmeh S, Awad M, Al-Betar MA, Al-Redhaei A. Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified arithmetic optimization algorithm. Internet Things. 2023;22(2):100819. doi:10.1016/j.iot.2023.100819.
59. Yin C, Zhu Y, Fei J, He X. A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access. 2017;5:21954–61. doi:10.1109/ACCESS.2017.2762418.
60. Arshad QUA, Khan WZ, Azam F, Khan MK, Yu H, Bin Zikria Y. Blockchain-based decentralized trust management in IoT: systems, requirements and challenges. Complex Intell Syst. 2023;9(6):6155–76. doi:10.1007/s40747-023-01058-8.
61. Gaber T, Awotunde JB, Folorunso SO, Ajagbe SA, Eldesouky E. Industrial internet of things intrusion detection method using machine learning and optimization techniques. Wirel Commun Mob Comput. 2023;2023(82):3939895. doi:10.1155/2023/3939895.
62. Zachos G, Mantas G, Porfyrakis K, Manuel Camões Sobral de Bastos J, Rodriguez J. Anomaly-based intrusion detection for IoMT networks: design, implementation, dataset generation, and ML algorithms evaluation. IEEE Access. 2025;13:41994–2028. doi:10.1109/ACCESS.2025.3547572.
63. Islam HMA, Khan KM, Maharaz MR, Antu AB, Billah F, Majumder S, et al. Revisiting ONE simulator in IoV research: seeing the forest through the trees. IEEE Access. 2025;13(2):50727–40. doi:10.1109/access.2025.3552026.
64. Mohapatra K, Singh D, Biswal AK. IoAT-based smart farming technology. In: Proceedings of the 2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA); 2023 Sep 29–30; Imphal, India. p. 585–90. doi:10.1109/ICIDeA59866.2023.10295169.
65. Allakaram Tawfeeq B, Masoud Rahmani A, Koochari A, Jafari Navimipour N. An improved evolutionary method for social Internet of Things service provisioning based on community detection. IEEE Access. 2024;12:132939–63. doi:10.1109/ACCESS.2024.3457672.
66. Khelloufi A, Ning H, Naouri A, Ben Sada A, Qammar A, Khalil A, et al. A multimodal latent-features-based service recommendation system for the social Internet of Things. IEEE Trans Comput Soc Syst. 2024;11(4):5388–403. doi:10.1109/tcss.2024.3360518.
67. Singh Popli M, Singh RP, Kaur Popli N, Mamun M. A federated learning framework for enhanced data security and cyber intrusion detection in distributed network of underwater drones. IEEE Access. 2025;13:12634–46. doi:10.1109/ACCESS.2025.3530499.
68. Aloraini F, Javed A, Rana O, Burnap P. Adversarial machine learning in IoT from an insider point of view. J Inf Secur Appl. 2022;70(3):103341. doi:10.1016/j.jisa.2022.103341.